

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF
INFORMATION STORED AT PREMISES
CONTROLLED BY GOOGLE LLC AND
ASSOCIATED WITH THE FOLLOWING
EMAIL ADDRESSES:

BOOOKFAR@GMAIL.COM,
CC.STORE52@GMAIL.COM,
CHEWSDAWN@GMAIL.COM,
FA451183@GMAIL.COM,
GILBERTPACE47@GMAIL.COM,
JOEYPIERRE460@GMAIL.COM,
KAYLASOSEXY4@GMAIL.COM,
KOLIEZBEN@GMAIL.COM,
KUWSHINBERTA@GMAIL.COM,
KWALFALL42@GMAIL.COM,
L3EBANG@GMAIL.COM,
LARRYFLLOYD40@GMAIL.COM,
LOUSJEFF7@GMAIL.COM,
M56PERRY@GMAIL.COM,
MERLUP26@GMAIL.COM,
MLARR4895@GMAIL.COM,
MORRE4861@GMAIL.COM,
PAUL.KICKER1977@GMAIL.COM,
ROCKETJOHNNYS@GMAIL.COM,
STAINEDCURRENCY@GMAIL.COM,
STUFF.101DUMPS@GMAIL.COM,
SUITELIFE3717@GMAIL.COM,
THEODORA12P@GMAIL.COM,
THRELARRY@GMAIL.COM,
TRAPYENZOE@GMAIL.COM,
VICKYLOWSIN@GMAIL.COM, AND
YAMSZOE@GMAIL.COM
TIARAMERCURIOS@GMAIL.COM

1:19-SW-312
1:19-SW-313
1:19-SW-314
1:19-SW-315
1:19-SW-316
1:19-SW-317
1:19-SW-318
1:19-SW-319
1:19-SW-320
1:19-SW-321
1:19-SW-322
1:19-SW-323
1:19-SW-324
1:19-SW-325
1:19-SW-327
1:19-SW-328
1:19-SW-329
1:19-SW-330
1:19-SW-331
1:19-SW-332
1:19-SW-333
1:19-SW-334
1:19-SW-335
1:19-SW-336
1:19-SW-337
1:19-SW-338
1:19-SW-339
1:19-SW-358

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
28 APPLICATIONS FOR 28 SEARCH WARRANTS**

I, Detective John Bamford, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of 28 Applications for 28 Search Warrants for certain information that is stored at premises controlled by Google LLC (Google), an electronic communications and/or remote computing service provider headquartered in 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in 28 Attachment As. This Affidavit is made in support of 28 Applications for 28 Search Warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) pertaining to the Google accounts that are further described in Section I of the 28 Attachment Bs (hereinafter, collectively, the “**TARGET ACCOUNTS**”). Upon receipt of the information described in Section I of the Attachment Bs, government-authorized persons will review that information to locate the items described in Section II of the Attachment Bs.

2. I am a Detective with Arlington County Police Department (ACPD) and am currently a Task Force Officer with the Federal Bureau of Investigation (FBI). I am assigned to the Cyber Crime Squad of the Washington Field Office. I have been employed by ACPD since 2008. In the course of conducting or participating in criminal investigations, I have been involved in interviewing and debriefing witnesses and informants; conducting physical surveillance; tracing and analyzing internet protocol addresses; tracing and analyzing financial transactions; analyzing telephone pen registers; collecting and analyzing evidence; and preparing and executing search warrants.

3. The facts in this Affidavit come from my personal observations, training and experience, and information obtained from other agents and witnesses. This Affidavit is

intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience, and the facts stated herein, I respectfully submit there is probable cause to believe that violations of Title 18, U.S. Code, Sections 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud), 1343 (Wire Fraud), and 1349 (Wire Fraud Conspiracy) have been committed. Furthermore, there is probable cause to search the information described in the 28 Attachment As for evidence, instrumentalities, contraband, or fruits of these crimes as further described in the 28 Attachment Bs.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

A. Summary of the Investigation to Date

6. The investigation began in or around July 2018 after federal and state authorities discovered a pattern of fraudulent activity that appeared to be facilitated using a mobile application that serves as a “contactless” payment method. That is, individuals have been able to make fraudulent purchases linked to the payment accounts of victims who did not authorize the transactions, and have done so without swiping a physical payment card at a point-of-sale terminal or inserting a physical payment card into a point-of-sale terminal.

7. I know from my training and experience that contactless payments can be achieved through cellular telephones. Purchasers can complete such transactions by associating

a payment card with a device capable of transmitting radio-frequency identifications (RFID) or near field communication (NFC) and then holding that device in close proximity to a point-of-sale terminal capable of accepting RFID or NFC transmissions. Perhaps the most well-known contactless payment systems are Apply Pay and Google Pay, which utilize NFC technology.

8. During the course of the investigation, I have discovered that third-party applications that allow for NFC contactless payments are available for purchase and/or download within the Google Play Store.

9. Law enforcement, through its investigation, has identified one of the participants of this criminal scheme as Merlin Laguerre, who made numerous fraudulent purchases in retail stores in the Eastern District of Virginia and was captured on surveillance footage carrying out the transactions using what appeared to be a mobile phone held in close proximity to a point-of-sale terminal at those retail stores. Laguerre was subsequently charged in the Eastern District of Virginia via indictment with one count of conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, two counts of wire fraud, in violation of 18 U.S.C. § 1343, and two counts of aggravated identity theft, in violation of 18 U.S.C. § 1028A. *See United States v. Laguerre*, No. 1:19-cr-15 (E.D. Va.).

10. On March 13, 2019, Laguerre entered a guilty plea to one count of wire fraud conspiracy, one count of wire fraud, and one count of aggravated identity theft, and he currently is awaiting sentencing. Laguerre, as part of his guilty plea, admitted that, from at least in or around October 2016 through at least September 2018, he conspired with others to enrich themselves by obtaining and using stolen payment card information, as well as stolen personally identifying information (PII). Laguerre also admitted that he and his co-conspirators, at times, trafficked in stolen payment card information, at other times fraudulently opened lines of credit,

and at other times used stolen payment card information to make fraudulent purchases at retail stores. Markedly, Laguerre admitted that, on occasion, he communicated with his co-conspirators via a messaging platform known as ICQ.

11. Laguerre initially was apprehended in or around September 2018 by law enforcement officers with the Henrico County Police Department. At the time of his apprehension, law enforcement seized, pursuant to search warrants issued by a magistrate judge of the Commonwealth of Virginia, a number of digital devices from both the vehicle Laguerre was driving and a hotel room in which Laguerre and his girlfriend were staying in Henrico County, Virginia. The FBI subsequently obtained a search warrant from the Honorable Theresa C. Buchanan on October 11, 2018, for those seized devices and conducted a digital forensic analysis.

12. As detailed below, evidence obtained from Laguerre's digital devices, combined with other sources, such as records from Google, indicate that the **TARGET ACCOUNTS** are controlled or used either by Laguerre's co-conspirators or close confederates of his criminal activity, and that the **TARGET ACCOUNTS** contain evidence of such criminal activity, as well as evidence of the identities of the individuals involved in the criminal conduct under investigation.

B. Identification and Arrest of Merlin Laguerre

13. On or about July 23, 2018, a representative of American Express (AmEx) contacted me and advised that, about a month earlier, on or about June 20, 2018, an AmEx credit card ending in 1004 (hereinafter, the "1004 card") had been used to make three unauthorized purchases at a Best Buy located at 1201 South Hayes Street in Arlington, Virginia, within the Eastern District of Virginia. These purchases totaled approximately \$8,968.

14. I subsequently went to the aforementioned Best Buy and spoke with a store supervisor. The store supervisor informed law enforcement of the following:

a. the individual who had made the fraudulent purchases on or about June 20, 2018, also had ordered an additional item, which was to be picked up at a Best Buy located in Alexandria, Virginia, within the Eastern District of Virginia;

b. the name associated with the item to be picked up was "Merlin Laguerre," and the associated telephone number and email were 718-781-6512 and jordanlagurre29@gmail.com, respectively; and

c. the aforementioned contact information was associated with additional orders at other Best Buy locations, including one order that was to be picked up at a Best Buy located at 3401 Jefferson Davis Highway, in Alexandria, Virginia, which also is within the Eastern District of Virginia.

15. Law enforcement thereafter contacted a Best Buy analyst who is a member of the company's Asset Protection Team, which is within the company's Security Department. The analyst provided law enforcement with a series of still photographs and video surveillance from multiple Best Buy stores, as well as receipts from June 20, 2018, that were associated with Laguerre's purchases. Surveillance images depicted an individual making purchases at three Best Buy stores on or about June 20, 2018. This individual was an African-American male, who appears to be approximately thirty years old, and who is wearing a backwards New York Yankee's baseball cap, dark Adidas pants, white and grey shoes, and a New York Yankee's jersey on the back of which there is the number 22 and name "Ellsbury."

16. Subsequently, law enforcement obtained additional records from Best Buy, which included surveillance images depicting the same individual described in Paragraph 15 at a point-

of-sale terminal in a Best Buy store and placing a phone near the point-of-sale terminal's NFC reader.

17. I also learned through the investigation that Henrico County Police Department (HCPD) received similar information from AmEx about fraudulent purchases at area stores and undertook its own investigation. HCPD has related the evidence it gathered, consisting of transaction records and surveillance images, and a review of that evidence shows that a man matching the description of the individual discussed above had engaged in similar fraudulent activity at other Apple and Best Buy stores in Henrico County, Virginia, in or around June 2018.

18. Then, on or about September 5, 2018, HCPD received information about a stolen payment card number being used to pay for Room 113 at the Residence Inn by Marriott located at 2121 Dickens Road in Richmond, Virginia. HCPD thereafter discovered that the payment card number in question was owned by an individual, who will be identified herein as "W.B.," and had been used without W.B.'s authorization. As a result, Detective David Monticelli, who was the lead HCPD investigator for the fraud transactions in Henrico County described above, went to the hotel. Det. Monticelli was not in full uniform.

19. Det. Monticelli obtained reservation records from the hotel, which showed that Room 113 was to be rented from on or about August 27 to September 8, 2018. The reservation records also showed that the room had been rented under the name of "Merlin Laguerre." Reservation records further indicated that jordanlaguerre29@gmail.com had been provided as an email address.

20. Staff at the hotel advised Det. Monticelli that the individual renting Room 113 was an African-American man. Staff further advised that this individual was with an African-American woman and was utilizing a white, mid-sized SUV.

21. At approximately 8:10 a.m. on or about September 6, 2018, Det. Monticelli, who was in an unmarked police vehicle, was in the parking lot of the Residence Inn when he saw a white SUV pulling into the parking lot. Det. Monticelli observed that an African-American man was driving the vehicle and that an African-American woman was in the front passenger seat of the vehicle. In light of the information provided by the hotel, Det. Monticelli concluded that the occupants of the vehicle likely were the individuals involved in the fraudulent reservation of Room 113. Det. Monticelli, as a result, requested assistance from uniformed officers.

22. In observing the SUV, Det. Monticelli noted that the individuals within the vehicle seemed to be delaying their exit from it. He concluded from this observation that it was likely the individuals had spotted him and suspected he was a law enforcement officer. According to Det. Monticelli, the woman in the SUV eventually exited the vehicle and proceeded to go to Room 113. Det. Monticelli observed that the woman was unable to enter the room, however. (This was because hotel management had changed the lock to the room as a result of the fraudulent payment provided for the room.) Det. Monticelli then saw the woman go back to the vehicle.

23. Next, Det. Monticelli saw the man in the SUV exit the vehicle and begin to walk toward the rental office. Det. Monticelli then drove past the man in order to get a better look at him. Based on this observation of the man, Det. Monticelli came to believe that the man was the same individual depicted in Best Buy's and Apple's surveillance footage that had been provided to HCPD. Det. Monticelli also saw that the man was talking on a cell phone and then was picked up by the same white SUV that Det. Monticelli had seen earlier.

24. Det. Monticelli proceeded to follow the SUV until it could be stopped by law enforcement officers in marked police patrol vehicles. At the time of the stop, the two

individuals had switched places within the vehicle compared to when they were observed pulling into the hotel parking lot; that is, the woman was now driving the vehicle and the man was in the front passenger seat.

25. During the next series of events, Det. Monticelli and HCPD were involved in two scenes which they undertook at approximately the same time. One group of individuals was at the scene of the car stop while the other group executed the search of Room 113 pursuant to a warrant. Det. Monticelli was involved in both and was the primary investigator.

The Stop of the White SUV

26. At approximately 8:15 a.m. HCPD police patrol vehicles stopped the SUV at Det. Monticelli's request. The HCPD law enforcement officers involved in the car stop soon discovered that an odor was emanating from the vehicle, and that, consistent with their training and experience, the odor appeared to be of marijuana. Law enforcement officers took the man, who was riding in the front passenger seat, into custody, and later identified the man as Laguerre and determined that he had been driving the vehicle earlier with a suspended driver's license. Also removed from the vehicle was the female driver, Nejah Foy.

27. HCPD law enforcement officers then conducted a search of the vehicle based upon both the smell of marijuana coming from the vehicle and also based upon probable cause that its occupants were engaged in the fraudulent activities described above. They discovered within the vehicle a silver Acer laptop computer and three cellular telephones. The Acer laptop was found in the backseat of the vehicle in a small bag. A ZTE cellular phone was located within the center console of the vehicle, a Samsung Galaxy S9 cellular phone was located in the front passenger seat, and an Apple iPhone S cellular phone was located inside a clothing bag within the back of the vehicle. Also, located within the clothing bag was a Lanora LNR820 magnetic

stripe reader/writer. HCPD would later discover a magnetic reader/writer of the same make and model within the hotel room.

28. At the scene of the car stop, Det. Monticelli provided Laguerre with a verbal *Miranda* warning and Laguerre stated that he understood his rights. Det. Monticelli asked Laguerre if he had been to any Best Buy or Apple stores located at the Short Pump Town Center in Richmond in the past six months and Laguerre stated he had not been into the stores.

29. Det. Monticelli also interviewed Foy. This interview occurred at the scene of the car stop. Foy identified herself as Laguerre's girlfriend for the last three months and stated that they had just arrived back from New York where they had been visiting family.

30. Later on or about September 6, 2018, Det. Monticelli had another voluntary interview with Foy. During this interview, Det. Monticelli showed Foy a number of stills from the surveillance footage that Best Buy and Apple had provided in connection with fraudulent transactions occurring in June 2018 in or around Henrico County. Foy identified the man depicted in the photographs as Laguerre. Foy also admitted to obtaining an Apple laptop from a Best Buy store located in or around the Midlothian Turnpike, and stated that she gave the laptop to Laguerre. Foy, however, did not have any more information about the laptop's whereabouts.

The Search of Room 113

31. HCPD obtained two search warrants for Room 113, authorizing the search and seizure of evidence of certain violations of the Code of Virginia. The first search warrant was obtained on or about September 5, 2018, and concerned violations of Virginia Code §§ 18.2-192 (Credit Card Theft), and 18.2-193 (Credit Card Forgery). A second, supplemental search warrant was obtained on or about September 6, 2018, due to the discovery of a credit card embosser discovered in Room 113. This second warrant authorized the search and seizure of evidence of

violations of Virginia Code §§ 18.2-192 (Credit Card Theft), 18.2-193 (Credit Card Forgery), and 18.2-185 (Credit Card Fraud; Conspiracy).

32. According to HCPD, during the search of Room 113, law enforcement discovered the following items:

a. a Wonder Embosser Machine, which, I know, based upon my training and experience, is an embosser machine commonly utilized to create fraudulent payment cards by imprinting physical cards with raised lettering in order to make the cards appear to be legitimate and which was found in a front hall closet;

b. a Lanora LNR820 magnetic stripe reader/writer, which, I know, based upon my training, experience, and open source research, can be utilized to encode stolen payment card numbers onto physical payment cards and which was found in the same front hall closet;

c. a Kyocera cellular phone and an Alcatel cellular phone found in the same front hall closet;

d. various electronic devices, including, within a backpack located in the main closet of Room 113's living area, a MSI Red and Black laptop, a red and silver thumb drive, and a 256MB SIM card.

33. HCPD also reports that it discovered what are believed to be fraudulently encoded payment cards. Law enforcement compared the numbers on the front of the cards to the number encoded on the cards' magnetic stripes and determined that, for two of the cards, the numbers did not match. Moreover, according to HCPD, many of the cards were embossed with the name "Merlin Laguerre."

34. The FBI subsequently determined that two of the aforementioned cards had been issued by AmEx, and thereafter contacted AmEx about the card numbers, one card ending in 1007 and the other ending in 3003. According to AmEx, none of the numbers found on the magnetic stripes of the cards had been issued to Laguerre, and instead were associated with accounts belonging to other individuals.

C. Additional Information Obtained by Henrico Law Enforcement

35. HCPD law enforcement has related that, during the course of its investigation, it learned that a few days earlier, on or about September 2, 2018, the first card utilized to pay for Room 113 was a “chargeback.”¹ Law enforcement learned that the manager of the hotel, M.C., went to the room, observed luggage still in the room, and assumed that the room remained occupied.

36. M.C. then called the person who had reserved the room, Merlin Laguerre, regarding the “chargeback.” According to M.C., Laguerre stated that he was out of town but would be returning. Laguerre provided M.C. a new payment card number to pay for the room but this number failed to clear. M.C. then asked Laguerre for a different number, at which point M.C. heard Laguerre ask an unknown individual, “hey girl, can I use your number?” Laguerre then provided M.C. with a third payment card number. (This number was the payment card number owned by W.B.)

¹ I know from my training and experience that a “chargeback” is when a payment card provider demands that a retailer, merchant, or other seller of good or services pays back the loss accrued by a payment card provider due to the retailer/merchant/seller accepting a fraudulent payment card.

37. According to M.C., W.B. called the hotel approximately two hours after the number provided by Laguerre went through the hotel's payment system. M.C. asked W.B. if Laguerre was known to W.B., and W.B. replied in the negative.

D. Review of the Kyocera Phone and Discovery

38. On or about October 11, 2018, the Honorable Theresa C. Buchanan issued a search warrant authorizing federal law enforcement to search the devices seized by HCPD during Laguerre's arrest and from his hotel room and vehicle for fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), and 1349 (Conspiracy to Commit Wire and Bank Fraud) involving Laguerre or Foy.

39. A forensic analysis on the Kyocera phone was conducted and it revealed that the jamesbest881888@gmail.com and charlesmason722@gmail.com had received emails via the phone seized. Markedly, some of the emails sent to these addresses were addressed to Laguerre and pertained to e-currency transactions:

a. For example, an email was sent to jamesbest881888@gmail.com on or about February 6, 2018. This email was sent from *xcoins.io* and stated in relevant part, "Dear Merlin Laguerre, This is your email confirmation code."²

b. In addition, on or about February 13, 2018, another email was sent to jamesbest881888@gmail.com from *xcoins.io*. This email again started "Dear Merlin Laguerre," and then stated in relevant part, "a lender is now available for your bitcoin loan."

c. Similarly, an email was sent on or about February 14, 2018, to

² I know from my training and experience that *xcoins.io* is an online forum that advertises itself as being a website that allows individuals to purchase bitcoin.

charlesmason722@gmail.com from Edible Arrangements confirming an order for approximately \$340.94. Although the order purportedly was placed by Charles Mason with a MasterCard ending in 3726, the order lists Laguerre as the person who is to pick up the order and gives the phone number of 718-781-6512, which is the same number provided to Best Buy as noted above in Paragraph 14(b).

40. Analysis of the Kyocera also revealed evidence of Google Drive accounts linked to jamesbest81888@gmail.com, charlesmason720@gmail.com, and jordanlaguerre29@gmail.com.

41. Analysis of the phone also shows numerous conversations related to the obtaining and passing of what are believed to be stolen payment card numbers. Some of these conversations occurred in the messaging phone application known as ICQ,³ and involved the exchange of what appears to be stolen payment card information as well as PII of presumably the payment card account holder. Some of these communications also appear to concern e-currency wallets. I know that e-currency, or “virtual currency,” is a common way that individuals pay for stolen payment card information and that the exchanging of e-currency wallets allows for such payments to be made.

E. Review of Google Records Received Pursuant to a § 2703(d) Order.

42. On October 15, 2018, the Honorable Theresa C. Buchanan issued an Order pursuant to 18 U.S.C. § 2703(d) for certain account information pertaining to jordanlaguerre29@gmail.com and jordanlaguerre126@gmail.com. Google produced records for

³ I know from my training and experience that ICQ is an instant messaging service that can operate on electronic devices, such as phones with the capability of connecting to the Internet.

these accounts, and a review of those records revealed the following connections to jordanlaguerre29@gmail.com:

a. A Kyocera cellular phone with IMEI number 014400004636649 was utilized to access jordanlaguerre29@gmail.com. This same cellular phone also was linked, per Google's records, to the accounts of charlesmason722@gmail.com and jamesbest881888@gmail.com.

b. A Samsung SM-G960U cellular phone also was used to access jordanlaguerre29@gmail.com, which is notable because a Samsung phone of this make and model was among the devices seized by law enforcement at or around the time of Laguerre's arrest.

c. A Samsung SM-G960U with IMEI number 356915090589317 was used to access the email account of rozeblack41@gmail.com, which is notable because a Samsung phone of this make and model and with this particular IMEI number was among the devices seized by law enforcement at or around the time of Laguerre's arrest. The date of last "check-in" recorded by Google, which keeps information as to when a Google account was last accessed on a particular device, was September 5, 2018, the day prior to Laguerre's arrest by Henrico County Police.

d. Google permits users to associate a phone number with their accounts and Google's records show that 917-724-1220 was the number provided for jordanlaguerre29@gmail.com, as well as the following accounts: vyviane1988@gmail.com; shameerhaniff1988@gmail.com; bentracks123@gmail.com; margaretmiles8891@gmail.com; octaviathedgpeeth1988@gmail.com; and vivyane1988@gmail.com. Based on phone subscriber records that law enforcement obtained, it was determined that 917-724-1220 was registered to

Laguerre. Thus, there is good reason to believe that Laguerre controls and/or uses all of those email addresses.

e. The account rozeblack41@gmail.com was linked to the account of jordanlaguerre29@gmail.com via phone number 929-395-2995, which was listed as a method of contact in both accounts. Based on my experience and training, the fact that these accounts are linked by the same phone number strongly indicates that both email accounts are controlled and/or used by the same person, *i.e.*, Laguerre.

43. Also, discovered within the review of the Google records was email header information that showed the date an email was transmitted from jordanlaguerre29@gmail.com or the date the email account received an email, as well as the email addresses corresponded with. One of the notable email headers found was a header email was sent on or about July 27, 2018, from no-reply@coinbase.com to jordanlaguerre29@gmail.com. According to Coinbase's website, Coinbase "is a digital currency wallet and platform where merchants and consumers can transact with new digital currencies like Bitcoin, Ethereum, and Litecoin." In my training and experience, individuals who utilize stolen payment card numbers often use e-currency exchanges, such as Coinbase, to further their criminal actions. For example, Internet sites that sell stolen payment card information typically require purchasers to buy the information using e-currency, such as those commonly sold by Coinbase. Furthermore, based upon my training and experience I know that individuals involved in criminal acts, such as the usage of stolen payment card information, often will convert the proceeds of their criminal acts into e-currency, such as those sold by Coinbase. This conversion from fiat to e-currency allows criminals to effectively launder the proceeds of their criminal acts.

F. Search Warrant Return for Various Email Accounts

44. On December 7, 2018, the Honorable Michael S. Nachmanoff issued a search warrant authorizing the search and seizure of jordanlaguerre29@gmail.com and nine additional Google accounts that had been tied to jordanlaguerre29@gmail.com, as described above, for fruits, evidence, contraband, or instrumentalities of violations of 18 U.S.C. §§ 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), and 1349 (Conspiracy to Commit Wire and Bank Fraud) involving Laguerre or his co-conspirators. Specifically, the accounts that were the subject of the search warrant were vyviane1988@gmail.com, shameerhaniff1988@gmail.com, bentracks123@gmail.com, jordanlaguerre29@gmail.com, margaretmiles8891@gmail.com, octaviashedgepeth1988@gmail.com, vivyane1988@gmail.com, rozeblack41@gmail.com, jamesbest881888@gmail.com, and charlesmason722@gmail.com.

45. Google subsequently produced records pertaining to the aforementioned accounts. Analysis of these records resulted in the discovery of over 4,000 suspected payment card numbers sent among a number of the accounts.

46. Then, on January 24, 2019, the Honorable Theresa C. Buchanan issued a search warrant authorizing the search and seizure of various records associated with 10 Google accounts that had corresponded with the 10 Google accounts that were the subject of the December 7, 2018 search warrant about stolen payment card information or an individual believed to be involved the trafficking of such information or otherwise had been linked to those accounts via common phone numbers or devices. The accounts that were the subject of that warrant, which authorized the search and seizure of fruits, evidence, contraband, or instrumentalities of violations of 18 U.S.C. §§ 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud),

1343 (Wire Fraud), 1344 (Bank Fraud), and 1349 (Conspiracy to Commit Wire and Bank Fraud) involving Laguerre or his co-conspirators, were koleya40@gmail.com, sanotrah@gmail.com, mbuttler1985@gmail.com, bentracks6@gmail.com, richardpacella75nc@gmail.com, hardwickmaryssa@gmail.com, archietracy29@gmail.com, deidraroper65@gmail.com, angelidelfonsodr@gmail.com, lateishaedmonds2018@gmail.com, benbarthelus28@gmail.com, selenalucrez@gmail.com, rbarthelus81@gmail.com, and kencasey1977@gmail.com.

47. Google subsequently produced records pertaining to the aforementioned accounts.

A review of those records revealed a number of instances in which suspected payment card numbers were sent to or from one of the aforementioned accounts and one of the **TARGET ACCOUNTS**, such as the examples provided in the table below:

Date (On or About)	Sending Account	Receiving Account
Mar. 15, 2014	selenalucrez@gmail.com	T.CRAFTMAN848@GMAIL.COM
Mar. 13, 2015	ROCKETJOHNNYS@GMAIL.COM	selenalucrez@gmail.com
Nov. 17, 2015	selenalucrez@gmail.com	STAINEDCURRENCY@GMAIL.COM
Dec. 7, 2015	selenalucrez@gmail.com	YAMSZOE@GMAIL.COM
Sept. 17, 2016	selenalucrez@gmail.com	BIGBALLAG09@GMAIL.COM
Sept. 22, 2016	SUITELIFE3717@GMAIL.COM	selenalucrez@gmail.com
Oct. 29, 2016	selenalucrez@gmail.com	TRAPYENZOE@GMAIL.COM
Dec. 16, 2016	KWALFALL42@GMAIL.COM	koleya40@gmail.com
Jan. 5, 2017	LARRYFLLOYD40@GMAIL.COM	koleya40@gmail.com
July 7, 2017	JOEYPIERRE460@GMAIL.COM	sanotrah@gmail.com
Aug. 18, 2017	L3EBANG@GMAIL.COM	sanotrah@gmail.com
Sept. 27, 2018	BOOOKFAR@GMAIL.COM	sanotrah@gmail.com

48. Furthermore, within the records provided by Google, law enforcement discovered communications that appear to relate to the exchange of stolen payment card information, such as the examples provided below:

a. On or about December 4, 2015, koleya40@gmail.com sent an email to **STUFF.101DUMPS@GMAIL.COM** asking, "hey wassuo bro can I get ur icq to make an

order[?]" I know from my training and experience that the word "dumps" is terminology commonly used by individuals engaged in the sale of stolen payment card numbers to refer to the data found on the magnetic stripe of a payment card. I also know from my training and experience that the term "order" can, in the context of trafficking in stolen payment card information, refer to the purchase of stolen payment card information.

b. On or about July 12, 2018, an email was sent from **KUWSHINBERTA@GMAIL.COM** with the subject line of "SuperMario Dumps Shop !!!". This email was sent to various accounts to include the account of **selenalucrez@gmail.com**. This email states in relevant part "i know from my friend that you are a good buyer of dumps maybe you want to try my shop too, we got best valid rate,best [sic] customers support and also we will give you bonus first time you will load." The email includes a website address for what appears to be a website associated with Super Mario Dumps.

c. On or about November 9, 2018, **PAUL.KICKER1977@GMAIL.COM** sent an email to **sanotrah@gmail.com** with the subject line, "Super Mario Dumps New Domain !!!" The email states in relevant part that the website address for Super Mario Dumps has changed.

d. On or about May 20, 2017, **CC.STORE52@GMAIL.COM** sent an email to **selenalucrez@gmail.com** that stated in relevant part, "I wanna present automated secure dumps shop service with high quality dumps."

e. On or about May 27, 2016, **CC.STORE52@GMAIL.COM** sent another email to **selenalucrez@gmail.com**. The email contained a link to **www.king-dumps.us** and indicated that this site was "heaven of dumps with pin."

49. The records provided by Google also revealed a number of the **TARGET**

ACCOUNTS linked to each other and the accounts that were the subject of the January 24, 2019, such as the examples provided below:

- a. The recovery email for sanotrah@gmail.com was listed as **THEODORA12P@GMAIL.COM**;
- b. **KAYLASOSEXY4@GMAIL.COM**, **TIARAMERCURIUS@GMAIL.COM**, **VICKYLOWSIN@GMAIL.COM**, and **CHEWSDAWN@GMAIL.COM** were associated with sanotrah@gmail.com based upon these accounts all having been logged into via the same cellular phone (*i.e.*, a Samsung SM-G530T1 with IMEI number 35913006437485);
- c. **GILBERTPACE47@GMAIL.COM** was associated with koley40@gmail.com based upon these accounts having been logged into via the same cellular phone (*i.e.*, a LGE LG-M210 with IMEI number of 353661087348795);
- d. **M56PERRY@GMAIL.COM** was associated with koley40@gmail.com based upon these accounts having been logged into via the same cellular phone (*i.e.*, a Samsung SM-J737T with IMEI number of 356058090544444); and
- e. **BOOOKFAR@GMAIL.COM**, **FA451183@GMAIL.COM**, **KOLIEZBEN@GMAIL.COM**, **LOUSJEFF7@GMAIL.COM**, **MERLUP26@GMAIL.COM**, **MLARR4895@GMAIL.COM**, **MORRE4861@GMAIL.COM**, **THRELARRY@GMAIL.COM**, and **VICKYLOWSIN@GMAIL.COM** were associated via cookies, small pieces of text sent to users' browsers by Google, which, based on my training and experience, indicate that the same device was used to access all of these accounts.

G. Use of Numerous Accounts by Cybercriminals

50. Through my training and experience, I am familiar with cybercrime actors using

numerous email accounts. Often times, they will create and use “criminal” accounts to make threats, obtain contraband, or commit fraud, while using and maintaining “legitimate” accounts to conduct lawful activities, such as registering for social media accounts open to the public.

51. However, in my training and experience, while criminal actors may attempt to keep their “criminal” and “legitimate” accounts separate, more often than not, there is comingling of information on the accounts, and thus, both “legitimate” and “criminal” accounts may contain evidence or constitute instrumentalities of crime. For instance, it is common for cybercriminals to forward contact information or records of fraudulent activity or profits gained from fraud from their “criminal” accounts to their “legitimate” ones. Moreover, as explained further below, communications and other information collected by Google in connection with the creation of a Google email account may provide crucial evidence of the identity of the user of that account and the “who, what, why, when, where, and how” of criminal activity under investigation. In other words there is probable cause not only to believe that the evidence, instrumentalities, and fruits of Laguerre’s and his co-conspirators’ crimes are stored within the **TARGET ACCOUNTS**, but that there is also probable cause to believe that user attribution evidence is stored within the accounts as well.

BACKGROUND CONCERNING GOOGLE

52. In my training and experience, and based on my review of Google’s website, terms of service, and privacy policy, I have learned the following about Google:

53. Google is a U.S. company that provides a variety of online services to the public. As described in further detail below, these services include, among many others, email, instant messaging, web searching, and file storage.

54. Google allows subscribers to obtain access to its services by registering for a

“Google Account.” A Google Account consists of a single username and password, and is uniquely associated with a Google email address, typically at the domain name “gmail.com,” like many of the Google Accounts listed in the Attachment As. Once a subscriber obtains a Google Account, the subscriber can use that same username and password to sign into any Google product. In other words, a Google Account username functions as a subscriber’s username across all of the dozens of Google services offered to the public. Google treats each account holder as a single user across all Google products. Google combines information that a user has provided from one service when signed in with information from other services.

55. Google asks subscribers to provide certain personal identifying information when registering for a Google Account. Such information includes the subscriber’s first and last name, date of birth, telephone number, other email address, and country of residence. In my training experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users. Based on my training and experience, I know that even if subscribers insert false information to conceal their identities, this information often provides clues to their identity, location, or illicit activities.

56. One of Google’s most popular services is Gmail, Google’s email service. Google allows subscribers to obtain email accounts at the domain name gmail.com. In general, an email (which can include attachments such as documents, images, and videos) that is sent to or from a Google subscriber, or stored in draft form in the account, is automatically stored in the subscriber’s Gmail account on Google servers until the subscriber deletes the email. If the subscriber does not delete a message from Gmail, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google’s servers for a certain period of time. A Gmail user can also store files in addition to emails, such

as address books, contact lists, user groups, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact lists, email in the account, and attachments to emails, pictures, and other files.

57. Another service offered by Google is called Google Maps, which provides users with a variety of records and tools related to maps and location. I know from my training and experience that, by default, Google Maps activity is associated with a user's Google Account, including all maps for which the user previously searched, records associated with custom maps created by or shared with the user, changes and edits to public places made by the user, starred places, private labels, and saved locations. Based on my training and experience, Google Maps can contain evidence of the user's location and identity. For example, a user will frequently save his home and/or work locations, and will "star" or favorite common destinations. A user who plans a robbery may search for the victim's location via Google Maps and may use Google Maps to get directions from the user's residence to the victim location, revealing both the user's address and specific planning steps taken in furtherance of the crime.

58. Google Drive is another Google service available to users with Google accounts. It allows users to create, store, edit, and share documents and other files. Google Drive encompasses various Office Suite applications, such as Docs (documents), Sheets (spreadsheets), and Slides (slide-based presentations). Files and documents stored in Google Drive are accessible from any smartphone, tablet, or computer, and can be shared with other users to view, edit or download. Google Drive files on a user's device will automatically "sync" with a user's Google Drive files on the web, so that a user can access and launch the same files from all of the user's devices. In general, a file on Google Drive is stored on Google servers until the subscriber

deletes the file. Even if the subscriber deletes the file, it may continue to be available on Google's servers for a certain period of time. In my training and experience, evidence of who was using a Google account, and evidence related to criminal activity of the kind described above, may be found in these files and records. For example, a user can use Google Drive to maintain a spreadsheet of incoming wire transfers and the related payments owed to co-conspirators.

59. A user's Google Drive may also contain back-up information from third-party apps. In some cases, such as with the messaging application WhatsApp, the back-up data is contained in a "hidden folder" which is inaccessible to the user. While Google may be able to produce the data, investigators may need to seek assistance from the third party behind the application in order to read or otherwise use the information.

60. Google offers a service through which a computer user can search webpages for text that the user enters. Under some circumstances, Google saves the user's text searches for later retrieval. Google also maintains Web History records for its users, recording information about the user's online activity. Web History records may include, among other things, the Google searches the user conducts, the web sites the user visits, and the videos the user watches. Google's Web and App Activity records for a user may similarly save the user's search activity on applications and browsers, including information about the websites the user visits; the applications that he uses; advertisements that the user clicks; and the user's location, language, and Internet Protocol address ("IP address"). This activity information can be saved even when the user is offline. Based on my training and experience, I am aware that a user's web and search history may include evidence of the crime itself as well as the user's identity and state of mind.

61. Google allows users to connect their Google Accounts to Chrome, Google's web browser. When a Google Account is signed into Chrome, all of the user's Chrome data, such as bookmarks, history, passwords, and other settings, are synched to the user's Google Account. The data is stored on Google's servers and made available to the user wherever he signs into Chrome, regardless of the device or location. Google may also keep records of the webpages or IP addresses that a user clicks on or types directly into his web browser's address bar if the user has logged into Google Chrome. For users of Google Chrome, Google may also save information that the user provided to third-party websites via forms filled out while logged into Chrome. This "Autofill" information may include the user's name, address, phone number, email address, and payment information. Based on my training and experience, information associated with Google Chrome may constitute evidence of the crime, as well as indicate the user's identity and location.

62. In my training and experience, in some cases, email account users may communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

63. In my training and experience, Google typically retains certain transactional information about the creation and use of each account on its systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*,

session) times and durations, the types of services utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account.

64. In addition, Google typically retains records of the IP address used to register the account and the IP addresses associated with particular logins to the account. IP address information can help to identify which computers or other devices were used to access the email account. Google also collects device-specific information (such as a subscriber's hardware model, operating system version, unique device identifiers, and mobile network information including phone numbers). Google may associate such device identifiers or phone numbers with a subscriber's Google Account. This information can show how, when, and from where the account was accessed or used. In my training and experience, I have learned that when the user of a mobile application installs and launches the application on a device (such as a cellular telephone), the application directs the device in question to obtain a Push Token, a unique identifier that allows the provider associated with the application (such as Google) to locate the device on which the application is installed. After the applicable push notification service (*e.g.*, Apple Push Notifications (APN) or Google Cloud Messaging) sends a Push Token to the device, the Token is then sent to the application, which in turn sends the Push Token to the application's server/provider. Thereafter, whenever the provider needs to send notifications to the user's device, it sends both the Push Token and the payload associated with the notification (*i.e.*, the substance of what needs to be sent by the application to the device). To ensure this process works, Push Tokens associated with a subscriber's account are stored on the provider's server(s). Accordingly, the computers of Google are likely to contain useful information that

may help to identify the specific device(s) used by a particular subscriber to access the subscriber's Google account via the mobile application

65. Information collected by Google also may assist investigators in linking multiple accounts to a single user or identifying other accounts associated with the user. Specifically, Google is able to identify other accounts accessed from the same computer (referred to as "cookie overlap"); accounts whose subscriber information includes same phone number or email address; and accounts where the same IP addresses were used to create or access the account in the same timeframe. This information can be used to further identify the user and to locate additional evidence of the criminal activity under investigation.

66. Further, Google maintains location history for its users. Google collects and processes an account holder's geographic location information when signed into Google services and maps those locations. Google can use a variety of information to determine location, including IP address and GPS. Google also may gather information regarding nearby devices, Wi-Fi access points, and cell towers. Location information may also be gleaned from Google services such as Google Maps.

67. The user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as geolocation, date and time) may indicate who used or controlled the account at a relevant time.

68. The logs, user attribution, and location information held by Google also allows investigators to understand the geographic and chronological context of access, use, and events

relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additional information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video).

69. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information in the account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime or map searches regarding the location that the crime was committed), or consciousness of guilt (*e.g.*, deleting communications or account information in an effort to conceal evidence from law enforcement).

70. As explained herein, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

71. There is reason to believe Google is still in possession of records related to the accounts. A preservation request was submitted electronically to Google requesting that, for a period of 90 days, Google "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process," pursuant to 18 U.S.C. § 2703(f). Google maintains and stores content and non-content data associated with an account for an extended period of time, potentially indefinitely if the account holder does not affirmatively delete the data. For example, an email that is sent to a Google subscriber is stored in the subscriber's inbox on Google's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely.

Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

72. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within the user-generated content created or stored by the Google subscriber. This type of evidence includes, for example, personal correspondence, personal photographs, purchase receipts, contact information, travel itineraries, and other content that can be uniquely connected to a specific, identifiable person or group. In addition, based on my training and experience, I know that this type of user-generated content can provide crucial identification evidence, whether or not it was generated close in time to the offenses under investigation. This is true for at least two reasons. First, people that commit crimes involving electronic accounts (*e.g.*, email accounts) typically try to hide their identities, and many people are more disciplined in that regard right before (and right after) committing a particular crime. Second, earlier-generated content may be quite valuable, because criminals typically improve their tradecraft over time. That is to say, criminals typically learn how to better separate their personal activity from their criminal activity, and they typically become more disciplined about maintaining that separation, as they become more experienced. Finally, because email accounts and similar Google accounts do not typically change hands on a frequent basis, identification evidence from one period can still be relevant to establishing the identity of the account user during a different, and even far removed, period of time


73. Based on my training and experience, I believe that data stored by Google in connection with the above services may contain evidence of the substantive crimes under investigation, as well as evidence of the account holders' geographic location and travel plans, the true identity and/or aliases of the account holders, and the location of financial assets subject

to seizure.

CONCLUSION

74. Based on the forgoing, I request that the Court issue the proposed Search Warrants.

Respectfully submitted,



John Bamford
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me
on this 18 day of April, 2019



/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Hon. Theresa C. Buchanan
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **BOOOKFAR@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **CC.STORE52@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **CHEWSDAWN@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **FA451183@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **GILBERTPACE47@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **JOEYPIERRE460@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with
KAYLASOSEXY4@GMAIL.COM that is stored at premises owned, maintained, controlled,
or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway,
Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **KOLIEZBEN@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **KUWSHINBERTA@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **KWALFALL42@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **L3EBANG@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with
LARRYFLLOYD40@GMAIL.COM that is stored at premises owned, maintained, controlled,
or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway,
Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **LOUSJEFF7@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **M56PERRY@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **MERLUP26@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **MLARR4895@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **MORRE4861@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with
PAUL.KICKER1977@GMAIL.COM that is stored at premises owned, maintained, controlled,
or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway,
Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with
ROCKETJOHNNYS@GMAIL.COM that is stored at premises owned, maintained,
controlled, or operated by Google LLC (Google), a company headquartered at 1600
Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with
STAINEDCURRENCY@GMAIL.COM that is stored at premises owned, maintained,
controlled, or operated by Google LLC (Google), a company headquartered at 1600
Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with
STUFF.101DUMPS@GMAIL.COM that is stored at premises owned, maintained, controlled,
or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway,
Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **SUITELIFE3717@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **THEODORA12P@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **THRELARRY@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **TRAPYENZOE@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **VICKYLOWSIN@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **YAMSZOE@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google LLC (Google), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with
TIARAMERCURIUS@GMAIL.COM that is stored at premises owned, maintained,
controlled, or operated by Google LLC (Google), a company headquartered at 1600
Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B

Particular Things to Be Seized

I. Information to Be Disclosed by Google (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any messages, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, any attachments associated with the emails, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. Any records pertaining to the user’s contacts, including address books, contact lists, or groups;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. A list of the types of Google service utilized and any dates associated with the commencement or termination of that use;

e. All records pertaining to devices associated with the Account and software used to create and access the Account, including device serial numbers, instrument numbers, model types/numbers, International Mobile Equipment Identities (IMEI), Mobile Equipment Identifiers (MEID), Global Unique Identifiers (GUID), Electronic Serial Numbers (ESN), Android Device IDs, phone numbers, Media Access Control (MAC) addresses, operating system information, browser information, mobile network information, information regarding cookies and similar technologies, and any other unique identifiers that would assist in identifying any such device(s), including unique application numbers and push notification tokens associated with the Account;

f. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any account (including both current and historical accounts) ever linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (*e.g.*, credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

g. Information regarding network identifiers from which any Google service was accessed, to include IP addresses and associated date and time of access;

h. All information held by Google related to an account holder's location and location history, including geographic locations associated with the user's account; IP addresses; GPS information; and information pertaining to nearby devices, Wi-Fi access points, and cell towers;

i. The contents of all Google Drive files associated with the account, and logs pertaining to use and access of those files, including Sheets, Docs, Slides, Forms, and Drawings;

files stored by the account; files shared with or by the account and the account with or by whom the files were shared; the accounts or email addresses associated with each file use or access; the date and time at which each file was stored, shared, accessed, or edited; and the size and type of each file;

j. All Google Maps data, including all Maps information associated with a user's search history; records associated with custom maps created by or shared with the user; the identity of other accounts with which the user shared said maps; changes and edits to public places; starred places, private labels, and saved locations; and the logs and metadata associated with all of the above;

k. The text of all Internet search requests input by the subscriber; the contents of any Chrome data associated with a user's account, to include bookmarks, passwords, and history; any saved autofill information; and all URLs or IP addresses typed into the Google Chrome address bar or URLs or IP addresses clicked on;

l. All records pertaining to communications between Google or its representatives and any person regarding the account, including contacts with support services and records of actions taken; and

m. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to Be Seized by the Government

All information and records described above in Section I that constitutes fruits, evidence, contraband, or instrumentalities of violations of Title 18, U.S. Code, Sections 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud), 1343 (Wire Fraud), and 1349 (Wire Fraud Conspiracy), and involve MERLIN LAGUERRE or his co-conspirators, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. documents, communications, or other information relating to the obtainment, purchase, sale, transmission, or use of identities or personally identifying information (including names, Social Security numbers, birth dates, payment card numbers, or bank accounts) or financial information associated with individuals other than LAGUERRE or his co-conspirators;

b. documents, communications, or other information relating to the obtainment, purchase, sale, transmission, or use of fake or falsified personally identifying information (including names, Social Security numbers, birth dates, payment card numbers, or bank accounts) or financial information;

c. documents, communications, or other information relating to the transferring or attempted transferring of money via e-currency or by wire, between bank accounts and/or by or between credit card processing accounts, including the nature, source, destination, and use of those funds;

d. documents, communications, or other information relating to the obtainment, purchase, sale, transmission, or use of stolen, falsified, or fake payment card numbers;

- e. documents, communications, or other information relating to the structuring or other concealment of financial transfers and/or withdrawals, including e-currency;
- f. lists or ledgers of payment card numbers issued by financial institutions or credit card companies to customers of those financial institutions or credit card companies (other than LAGUERRE or his co-conspirators);
- g. lists, ledgers, or other information memorializing items purchased fraudulently (including the types of items, amounts paid, and payment information used), as well as the dates and places of transactions;
- h. identity documentation, such as visas, passports, driver's licenses, birth certificates, and immigration records;
- i. bank records, checks, credit card bills, account information, and other financial records;
- j. documents, communications, and other information regarding LAGUERRE's or his co-conspirators' schedule or travel;
- k. communications with victims, credit companies, financial institutions, e-currency companies or vendors, or merchants or retailers;
- l. photographs of LAGUERRE or co-conspirators involved in the criminal conduct identified above, or that would reveal the identity or relationships between co-conspirators;
- m. documents, communications, and other information regarding the usernames, phone numbers, emails, or social media or instant messenger names used by LAGUERRE or his co-conspirators to transmit victims' personally identifying information, payment card numbers, and false identification documents;

n. documents, communications, and other information indicating the state of mind as it relates to the crime under investigation of LAGUERRE and his co-conspirators;

o. documents, communications, and other information, including address or telephone books or contact lists, that reflect names of potential criminal associates involved in the crimes under investigation;

p. documents, communications, and other information regarding the identity of co-conspirators, accomplices, and aiders and abettors in the commission of the criminal activity under investigation, including information that reveals their whereabouts;

q. documents, communications, and other information indicating how and when each account or identifier listed on Attachment A was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

r. documents, communications, and other information indicating the state of mind of the owner of each account or identifier listed on Attachment A as it relates to the crime under investigation;

s. the identity of the person(s) who created or used each account or identifier listed on Attachment A, including records that help reveal the whereabouts of such person(s); and

t. documents, communications, and other information regarding the identity of the person(s) who communicated with each account or identifier listed on Attachment A about matters relating to the crimes under investigation, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC (Google), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature